视频资源

基础入门（P1-P5）

P1. 概念名词

**什么是域名？**

* 域名：是由一串用点分隔的名字组成的Internet上某一台计算机或计算机组的名称，用于在数据传输时对计算机的定位标识（有时也指地理位置）。

**什么是二级域名多级域名？**

* 二级域名：分两种
* 在国际顶级域名下的二级域名
* 国际顶级域名下二级域名， 二级域名一般是指域名注册人选择使用的网上名称，如“yahoo.com”；上网的商业组织通常使用自己的商标、商号或其他商业标志作为自己的网上名称，如“microsoft.com”。
* 国家顶级域名下二级域名
* 在国家顶级域名之下二级域名一般是指类似于国际顶级域名的表示注册人类别和功能的标志。例如，在“．com.cn”域名结构中，“.com”此时是置于国家顶级域名“.cn”下的二级域名，表示商业性组织，以此类推。

**域名发现对于安全测试意义**

* 可以给安全测试提供更多的测试点，方便获取更多相关信

1.2DNS

什么是DNS？

域名区域（domain name system）,域名和ip地址相互映射的一个分布式数据库，使人更方便访问互联网。DNS使用UDP端口53。对于每一级域名限制63字符，域名总长度235个字符。

**本地HOSTS与DNS的关系？**

**Hosts在本地将一些常用的网址域名与其对应的ip地址建立一个关联的“数据库”，当我们访问域名时，系统会首先自动从hosts文件中寻找对应的ip地址，找到打开网页，没有交DNS域名解析器进行ip地址的解析**

* Hosts地址：C:\Windows\System32\drivers\etc\hosts

**CDN是什么？与DNS的关系？**

**CDN是构建在数据网络上的一种分布式的内容分发网。可以提高系统的响应速度，也可以一定程度的拦截防御攻击**

**常见的DNS安全攻击有哪些？**

1. **缓存投毒：他是利用虚假internet地址替换掉域名系统表中的地址，进行破环**
2. **DNS劫持；在劫持的网络范围内拦截域名解析的请求，分析请求的域名，把审查以外的请求放行，否则返回假的ip地址或者什么都不做使请求失去响应，其效果就是对特定的网络不能访问或访问的是假地址。**
3. **DNS,DDOS攻击；通过控制大批僵尸网络利用真实DNS协议栈发起大量域名查询请求，利用工具软件伪造源ip发送海量DNS查询，发送海量DNS查询报文导致网络宽带耗尽而无法传送正常dns查询请求**

### 1.3 脚本语言

**常见的脚本语言类型有哪些？**

* asp php aspx jsp javaweb pl py cgi 等

**不同脚本类型与安全漏洞的关系？**

* 不同脚本可能爆发漏洞的可能性有所不同
* 不同脚本漏洞的存在点可能不同，因为不同语言的适用范围不同

**1.4后门**

**什么是后门？**

**通常指那些绕过安全性控制而获取或系统访问权的程序方法**

**2.在软件的开发阶段，程序员创建后门以便修改程序设计中的缺陷**

**后门在安全测试中的实际意义？**

**可以更方便的链接到主机**

**在获取到玩主机权限的时候，后门可以充当命令控制台的角色**

### 1.5 WEB

**WEB 的组成架构模型？**

* 网站源码：分脚本类型，分应用方向
* 操作系统：windows linux
* 中间件（搭建平台）：apache iis tomcat nginx 等
* 数据库：access mysql mssql oracle sybase db2 postsql 等

**为什么要从 WEB 层面为主为首？**

* web使用的比较广
* web网站了漏洞相对较多
* web 作为跳板深入到其他资源相对容易

### 1.6 WEB 相关安全漏洞

* WEB 源码类对应漏洞：SQL 注入，上传，XSS，代码执行，变量覆盖，逻辑漏洞，反序列化等
* WEB 中间件对应漏洞：未授权访问，变量覆盖...
* WEB 数据库对应漏洞：弱口令，权限提升...
* WEB 系统层对应漏洞：提权，远程代码执行
* 其他第三方对应漏洞
* APP 或 PC 应用结合类

**http协议**